

## National Aeronautics and Space Admin.

## § 1203.403

economic advantage relating to national security.

(h) Information of such nature that an unfriendly government in possession of it would be expected to use it for purposes prejudicial to U.S. national security and which, if classified, could not be obtained by an unfriendly power without a considerable expenditure of resources.

(i) Information which if disclosed to a foreign government would enhance its military research and development programs to the detriment of U.S. counterpart or competitive programs.

(j) Operational information pertaining to the command and control of space vehicles, the possession of which would facilitate malicious interference with any U.S. space mission, that might result in damage to the national security.

(k) Information which if disclosed could jeopardize the foreign relations or activities of the United States; for example, the premature or unauthorized release of information relating to the subject matter of international negotiations, foreign government information or information regarding the placement or withdrawal of NASA tracking stations on foreign territory.

(l) United States Government programs for safeguarding nuclear materials or facilities.

(m) Other categories of information which are related to national security and which require protection against unauthorized disclosure as may be determined by the Administrator. The Chairperson, NASA Information Security Program Committee, will promptly inform the Director, Information Security Oversight Office, General Services Administration (GSA) of such determinations.

[44 FR 34913, June 18, 1979, as amended at 48 FR 5890, Feb. 9, 1983]

### § 1203.401 Effect of open publication.

Public disclosure, regardless of source or form, of information currently classified or being considered for classification does not preclude initial or continued classification. However, such disclosure requires an immediate reevaluation to determine whether the information has been compromised to the extent that downgrading or declassification is indicated.

Similar consideration must be given to related items of information in all programs, projects, or items incorporating or pertaining to the compromised items of information. In these cases, if a release were made or authorized by an official Government source, classification of clearly identified items may no longer be warranted. Questions as to the propriety of continued classification should be referred to the Chairperson, NASA Information Security Program Committee.

### § 1203.402 Classifying material other than documentation.

Items of equipment or other physical objects may be classified only where classified information may be derived by visual observation of internal or external appearance, structure, operation, test, application or use. The overall classification assigned to equipment or objects shall be at least as high as the highest classification of any of the items of information which may be revealed by the equipment or objects, but may be higher if the classifying authority determines that the sum of classified or unclassified information warrants such higher classification. In every instance where classification of an item of equipment or object is determined to be warranted, such determination must be based on a finding that there is at least one aspect of the item or object which requires protection. If mere knowledge of the existence of the equipment or object would compromise or nullify the reason or justification for its classification, the fact of its existence should be classified.

### § 1203.403 State-of-the-art and intelligence.

A logical approach to classification requires consideration of the extent to which the same or similar information available from intelligence sources is known or is available to others. It is also important to consider whether it is known publicly, either domestically or internationally, that the United States has the information or even is interested in the subject matter. The known state-of-the-art in other nations

#### § 1203.404

is an additional substantive factor requiring consideration.

#### § 1203.404 Handling of unprocessed data.

It is the usual practice to withhold the release of raw scientific data received from spacecraft until it can be calibrated, correlated and properly interpreted by the experimenter under the monitorship of the cognizant NASA office. During this process, the data are withheld through administrative measures, and it is not necessary to resort to security classification to prevent premature release. However, if at any time during the processing of raw data it becomes apparent that the results require protection under the criteria set forth in this subpart D, it is the responsibility of the cognizant NASA office to obtain the appropriate security classification.

#### § 1203.405 Proprietary information.

Proprietary information made available to NASA is subject to examination for classification purposes under the criteria set forth in this subpart D. Where the information is in the form of a proposal and accepted by NASA for support, it should be categorized in accordance with the criteria of §1203.400. If NASA does not support the proposal but believes that security classification would be appropriate under the criteria of §1203.400 if it were under Government jurisdiction, the contractor should be advised of the reasons why safeguarding would be appropriate, unless security considerations preclude release of the explanation to the contractor. NASA should identify the Government department, agency or activity whose national security interests might be involved and the contractor should be instructed to protect the proposal as though classified pending further advisory classification opinion by the Government activity whose interests are involved. If such a Government activity cannot be identified, the contractor should be advised that the proposal is not under NASA jurisdiction for classification purposes, and that the information should be sent, under proper safeguards, to the Director, Information Security Oversight Office, General Services Adminis-

#### 14 CFR Ch. V (1–1–10 Edition)

tration, Washington, DC 20405, for a determination.

#### § 1203.406 Additional classification factors.

In determining the appropriate classification category, the following additional factors should be considered:

(a) *Uniformity within government activities.* The effect classification will have on technological programs of other Government departments and agencies should be considered. Classification of official information must be reasonably uniform within the Government.

(b) *Applicability of classification directives of other Government agencies.* It is necessary to determine whether authoritative classification guidance exists elsewhere for the information under consideration which would make it necessary to assign a higher classification than that indicated by the applicable NASA guidance. Generally, the classification by NASA should not be higher than that of equivalent information in other departments or agencies of the Government.

#### § 1203.407 Duration of classification.

(a) Information shall be classified as long as required by national security considerations. When it can be determined, a specific date or event for declassification shall be set by the original classification authority at the time the information is originally classified.

(b) Information classified under predecessor orders and marked for declassification review shall remain classified until reviewed for declassification under the provisions of the “the Order.”

[48 FR 5890, Feb. 9, 1983]

#### § 1203.408 Assistance by installation security classification officers.

Installation Security Classification Officers, as the installation point-of-contact, will assist installation personnel in:

(a) Interpreting security classification guides and classification assignments for the installation.

(b) Answering questions and considering suggestions concerning security classification matters.